Privacy Impact Assessment Frequently Asked Questions

1. What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is an analysis of how personal information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating personal information in an information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA process provides a means to assure compliance with applicable laws and regulations governing privacy.

2. What are the requirements that govern the conduct of PIAs at TRICARE Management Activity (TMA) , including Federal laws, regulations, and guidance; Department of Defense (DoD) regulations and guidance; and TMA policies?

The E-Government Act of 2002, Section 208
Office of Management and Budget (OMB) Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (dated September 26, 2003)
Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance Memorandum (dated October 28, 2005)
TRICARE Management Activity (TMA) Chief Information Officer (CIO) Memorandum on TMA Privacy Impact Assessments (PIAs) (dated February 10, 2006)

3. When is a PIA conducted?

Section 208 of the E-Government Act requires agencies to conduct a PIA before:

Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

4. Who completes a PIA?

The system owner and /or program manager completes a PIA. The system owners address how the data is used and who will use it.

5. What is information in identifiable form?

Information in Identifiable Form (IIF) is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Under Section 208 of the E-Government Act, when an electronic information system collects, manages or disseminates IIF from or about members of the public, that system must have a PIA.

6. How does TMA define Information Technology (IT)?

Information Technology (IT), as defined in the Clinger-Cohen Act , is any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

7. What are major information systems?

Major information systems include “large” and “sensitive” information systems. A major information system, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), is a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, or (v) significant role in the administration of an agency’s programs, finances, property or other resources.

8. What is a National Security System?

A National Security System, as defined in the Clinger-Cohen Act, is an information system operated by the Federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management

9. What is the PIA Online Tool?

The TRICARE Management Activity (TMA) has developed TMA PIA Online, a web-based tool, to assist in assessing TMA’s collection, management, and dissemination of information in identifiable form (IIF) accomplished through Military Health Systems (MHS) electronic information systems. The tool provides a methodology to complete a privacy impact assessment (PIA) on any IT system that handles IIF from or about members of the public. The E-Government Act, Office of Management and Budget (OMB) Memorandum 03-22, DoD PIA Guidance memo (dated October 28, 2005), and TMA require that privacy stakeholders, including program managers, system owners, Web site managers, information management staff, and/or system developers, collaborate to complete PIAs. The TMA program offices required to complete PIAs are the Resources Information Technology Program Office(RITPO), Clinical Information Technology Program Office (CITPO), and Executive Information and Decision Support (EI/DS). By using TMA PIA Online, privacy stakeholders can more easily prepare the PIA, generate a Summary PIA, and forward the PIA to the TMA Privacy Office for review, approval, reporting, and publication – all requirements of Congress, OMB, DoD and TMA.

10. How will training be made available?

Contact the Office of TMA Privacy email at PIAMail@tma.osd.mil. An office member will provide you with the training, guidance materials and answers you need to ensure your project has the Privacy safeguards it needs.